AO 106 (Rev. 04/10) Application for a Search Warrant HH

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple Ipad Pro Serial Number, DMPWG0FTHPT4, Apple Laptop Serial Number, C17N6MT86085, and Apple Iphone 12, Serial Number C392Q0T1N6XX, Currently in the possession of the Cincinnati FBI

Case No. 2:21-mj-24

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Production/advertising for child pornography in interstate commerce
18 USC 2422(b)	Coercion/enticement of a minor in interstate commerce
18 U.S.C. 2252	Receipt, distribution, and/or possession of visual depictions of a minor engaged in sexually explicit conduct in interstate commerce

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew D. McCabe, SA FBI
Printed name and title

Sworn to before me and signed in my presence. By video

Date: January 19, 2021

City and state: Columbus, Ohio Newark, Ohio XXXXXXXXXX

Elizabeth A. Preston Deavers
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF: Apple Ipad Pro Serial Number, DMPWG0FTHPT4, Apple Laptop Serial Number, C17N6MT86085, and Apple Iphone 12, Serial Number C392Q0T1N6XX, Currently in the Possession of The Cincinnati FBI	)	Case No. 2:21-mj-24
	)	Magistrate Judge:

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrew D. McCabe, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, Cambridge Resident Agency and I have been a Special Agent since September 2010. During my tenure as an FBI Special Agent, I have investigated numerous crimes including, but not limited to, bank robbery, drug trafficking, racketeering, kidnapping, violent extremism, and crimes against children.

2. While performing my duties as a Special Agent, I have participated in various investigations involving computer-related offenses and have executed search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. As part of my duties as a Special Agent, I investigate various criminal child exploitation offenses, including those in violation of 18 U.S.C. §§ 2251, *et seq* and 2421, *et seq*.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the following devices: 1) Apple iPad Pro Serial Number, DMPWG0FTHPT4; 2) Apple Laptop Serial Number, C17N6MT86085; and 3) Apple iPhone 12, serial number C392Q0T1N6XX (hereinafter the SUBJECT DEVICES). I have not withheld any evidence or information that would negate probable cause.

5. The SUBJECT DEVICES to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits and evidence of violations of 18 U.S.C. §§2251, 2252 and 2422(b) – the production, advertising/solicitation for/or, distribution, transmission, receipt, and/or possession of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography") and the coercion or enticement of a minor(s). I am requesting authority to search the entire content of the SUBJECT DEVICES, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or

advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

9. Title 18, United States Code, Section 2422(b), makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime. Production of child pornography as defined in 18 U.S.C. § 2251(a) is included in the definition of sexual activity for which any person may be charged with a crime.

10. As it used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

11. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

12. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

13. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.

14. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

15. "Computer"[1], as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

IV. BACKGROUND REGARDING DIGITAL DEVICES, THE INTERNET AND MOBILE APPLICATIONS

16. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

17. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit.

1 The term computer is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cell phones and tablet devices. Where the capabilities of these devices differ significantly from a traditional computer, they are discussed separately and distinctly.

These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

18. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

20. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets,

also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred, it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses[2] and other information both in computer data format and in written record format.

22. These internet-based communication structures are ideal for those seeking to find others

2 The IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. When mobile devices connect to the Internet they are assigned an IP address either by the residential/commercial WiFi ISP or the cellular ISP. The IP address assignments are controlled by the respective provider.

who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

23. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

24. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an

electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

26. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

27. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include Facebook Messenger, Text Now, KIK messenger service, and Instagram.

V. INVESTIGATION AND PROBABLE CAUSE

28. In approximately mid-January of 2020, your affiant received information from the Belmont County Sheriff's Office (BCSO) regarding an individual who had solicited nude photographs of two minor females residing in Belmont County. According to the information provided by BCSO, an adult female had turned herself into authorities in mid-January of 2019, in order to resolve various legal issues she had relating to prostitution and other similar activities. Once in the Belmont County jail, the female reached out to detectives regarding her concern about her minor daughters. The woman stated that when she had been engaged in prostitution, she had met a man named Bernhard Jakits online. She sent images of herself to Jakits, who lived in Maryland, in exchange for money that he sent her through Western Union. During her interactions with Jakits, he asked about her daughters, but she would divert the conversation away from them. However, according to the mother, her oldest daughter intercepted a text message from Jakits on the mother's phone while the mother was sleeping. It was shortly after this interaction that the mother turned herself into authorities, and, since she had left her phone in her home, she was concerned that her daughters had been in contact with Jakits.

29. As a result of the mother's statements, forensic interviews were conducted of the two daughters. The eldest daughter (hereinafter Victim 1), who was born in 2003 and was 15 years old at the time of the interview, revealed that she had sent nude photographs of herself to an adult male that she knew by the names Mr. Wow and Bernie. She further stated that she had informed Bernie of her age. According to Victim 1, Bernie had also tried to convince both her and her younger sister (hereinafter Victim 2, who was born in 2005 and was 13 years old at the time) to video chat with him in exchange for money. During the interview of Victim 2, she stated that she sent photos to a man that she knew as either Mr. Wow or Wild. She did not know his true name. She confirmed that Mr. Wow was aware of her age and the age of Victim 1, and that he solicited photos of them either nude or in their bras and underwear. Victim 2 admitted that she sent Mr. Wow three pictures of herself, including pictures of her nude, in exchange for money he had offered them. She also reiterated Victim 1's statement that Mr. Wow had sought to video chat with them in exchange for money, but that they had declined to do so. At the time of the interviews, the victims' guardian turned over three cellular telephones to BCSO which were believed to have been used to communicate with Jakits. Phone 1 was a pink i-Phone 8 belonging to Victim 1. Phone 2 was a Samsung Galaxy J7 Prime Cellular Telephone which belonged to Victim 1 and Victim 2's mother. Phone 3 was an Alcatel Tracphone Model A574BL which belonged to Victim 1 and Victim 2's grandmother and was utilized at times by Victim 2. A BCSO detective reviewed the contents of Phone 1, Victim 1's i-Phone phone, and confirmed that it contained several nude images of Victim 1 and Victim 2, images of them holding up school transcripts and or prescriptions that clearly showed their ages, and a chat thread with a contact named Mr. Wow, in which those images were sent and there were discussions about the money the girls would receive for such pictures. The chat thread listed the phone number for Mr. Wow as (443) 742-1792.

30. The BCSO identified the subject described by Victim 1, Victim 2 and their mother as a Bernhard Jakits, residing at 15 Spa Creek Landing, Annapolis, MD, 21403 by conducting an open source data base check on telephone number (443) 742-1792. In addition to their investigative reports detailing all of the foregoing information, BCSO provided your affiant with the three aforementioned cellular telephones.

31. On January 22, 2020, your affiant conducted an interview of the victims' mother to obtain further information regarding her interactions with Jakits. The mother self-admitted to being a prostitute and using the website, "Skip the Games," to meet clients. The mother's Skip the

Games profile included her photographs and a telephone number. On an unspecified date, Jakits contacted the mother and began an online relationship with her using the video messaging service Duo. Jakits sent money to the mother utilizing Western Union, and in exchange the mother sent Jakits photos and videos of her preforming sexually explicit activities. As the relationship between the mother and Jakits continued, Jakits would ask the mother to perform more degrading acts. When the mother refused, Jakits showed the mother images taken from her videos. Jakits stated he would send the photos to the mother's family member and other associates if she did not comply with his requests. In addition to photographs of the mother, Jakits showed her images he had of other women engaged in sexually explicit actions. In December 2018, Jakits learned the mother had two minor daughters. Jakits began asking the mother to introduce him to her daughters, Victim 1 and Victim 2. The mother informed Jakits that Victim 1 and Victim 2 were juveniles and he should not message them. After she turned herself into BCSO in January 2019, she received money on her books from a friend, which she knew to be Jakits. Also knowing that Jakits would not send her money for no reason, the mother became concerned about him communicating with Victim 1 and Victim 2. After a conversation with her daughters in which they confirmed they communicated with Jakits and sent him nude pictures in exchange for money, the mother reached out to BCSO detectives and provided this information. During the interview with your affiant, the mother identified a publicly available photograph of Bernhard Jakits obtained from roguewaveyachtsales.com website, as the man with whom she had been communicating. The website also listed (443) 742-1792 as Jakits' telephone number. The mother also provided consent to search the three aforementioned cellular phones. Your affiant thereafter submitted all three cellular phones to the FBI forensic examination laboratory and requested that they be forensically examined.

32. In January 2020, a subpoena was issued to Verizon wireless for subscriber information related to the phone number (443) 742-1792. Responsive information provided by Verizon identified the subscriber of (443) 742-1792 as Bernhard Jakits, P.O. Box 5015, Annapolis, MD.

33. In February of 2020, your affiant received and reviewed the forensic extractions of the three cell phones described in paragraph 14 above. During the review of the forensic extraction of Victim 1's pink i-Phone, your affiant observed 179 messages on the TextNow application exchanged between Victim 1 and the phone number 443-742-1792 that is associated with Jakits, between approximately January 14 and 21, 2019. The following are excerpts from the communications recovered from Victim 1's phone that occurred on or about January 14, 2019:

- VICTIM 1: This is [Victim 1]
- JAKITS: Then call me and I'll tell you.
- Four-minute call to Victim 1.
- JAKITS: Also important,,,Ask your sister if she wants to earn $500 also 8:00PM tonight Talk then.
- JAKITS: Got another idea Please call me.
- JAKITS: You there?
- VICTIM 1: I can't call I'm wit [sic] a friend now.
- JAKITS: Thanks for letting me know. Have fun. We'll speak later this evening. Remember to ask your sister.
- JAKITS: Hi....Did you ask your Sister yet?
- VICTIM 1: I'm at a friends staying the night so no I didn't ask her.
- JAKITS: Please ask her when you can And how about what we have planned for later
- VICTIM 1: It's still on
- JAKITS: Oh goodie
- JAKITS: Its almost 8pm dear
- JAKITS: [Victim 1][], I just sent your Mom more money to make her stay there a little more pleasant
- JAKITS: Its 8pm honey
- JAKITS: ???
- JAKITS: Did you fall asleep? I didn't...
- JAKITS: [VICTIM1][], you need to become a lot more responsible if you want my help
- VICTIM 1: I am responsible sometimes I'm just not in the mood to go through all this shit with u

34. The following are excerpts from the communication recovered from VICTIM1's phone that occurred on or about January 15, 2019:

- JAKITS: Are you up to making some money?
- JAKITS : $1000
- VICTIM 1: Yea

***

- JAKITS: Good When?
- VICTIM 1: When ever u want to
- JAKITS: 9:00pm sharp... Also, have you spoken to your sister, if so, $500 for her
- VICTIM 1: So how much am I getting and how much would she be if she said yes
- JAKITS: $1000 for your time $500 for your Sister's time
- VICTIM 1: Okay
- JAKITS: Okay what
- VICTIM 1: Okay as in we both r in
- JAKITS: Yes definitely I'd like to see what your sister looks like please

- VICTIM 1 sent Photograph 1, depicting two clothed minor females posing in front of a mirror, Photograph 2, depicting two clothed minor females lying on a bed, and Photograph 3, also depicting two clothed minor females lying on a bed, as text message attachments.
- VICTIM 1: She's the one with the curly hair
- JAKITS: Cute Very very cute both of you Before we start We need to promise that its our secret. This is as far as it goes...i promise Now one naked picture of your sister, after that we'll plan our party
- VICTIM1: Rn?

***

- JAKITS: Yes
- VICTIM 1 sent Photograph 4, an image of a young naked female holding a cellular phone. Both the female's breasts and pubic region are clearly visible.
- JAKITS: Well, whats happening? Plus with face of your sister
- VICTIM 1: I sent it
- JAKITS: Cute Have also show her school transcript Then you call me and i'll tell you what i want
- VICTIM 1: She hasn't got hers yet
- JAKITS: Have hold something up with her name on it
- VICTIM 1 sent Photograph 5 an image of a fully clothed female holding prescription from East Ohio Regional Hospital. The prescription shows VICTIM2's name and her date of birth
- JAKITS: Cute Now call me
- VICTIM 1 made a four-minute call to JAKITS.

***

- VICTIM1: What r u asking for on ft
- JAKITS: That she model and do certain things Nothing nasty I promise
- JAKITS: Plus a couple of pictures that i want her to take of how i want it
- VICTIM1: Okay

***

- JAKITS: It's 9 o'clock
- Incoming unanswered call to Victim 1 from Jakits
- VICTIM1: We're gonna have to wait a little longer my gma is in the room and someone is in the bathroom
- JAKITS: Hate waiting but i will

***

- VICTIM 1: So this is what we're doing . We're gonna do all the pictures first me and my sister and then we will ft so it can go faster and be over with
- JAKITS: Its not a bad plan You'll poise [sic] in the ways that i want you two to do Then if happy, we'll ft and finish it off How does that sound?
- VICTIM 1: Great
- JAKITS: Lets start sooner than later
- VICTIM 1: Waiting on u
- JAKITS: I'm here
- VICTIM 1: Okay so tell me the poses

- JAKITS: Call me and i'll tell you
- VICTIM 1: Just text me them I've got a lot of homework to do so I wanna do this quick
- JAKITS: First your sister Have her call me Don't want to write/text it
- JAKITS: Then you Tomorrow morning you guys will have $1500
- VICTIM 1 made a one-minute call to Jakits

***

- VICTIM 1: We don't rlly feel comfortable FaceTiming you so... idk
- JAKITS: $1500
- JAKITS: Its that or nothing I'm soon need to do other things, hope that you understand 1000 for you 500 for your sister Soon i'm leaving Because I have other obligations
- JAKITS: Facetime or google duo Its that or nothing

***

- JAKITS: One thousand five hundred dollars is a lot of money Think hard and long [Victim 1][]
- JAKITS: Remember that i can get more screwed with this than you can Yes or no or i'm going out Thanks either way

***

- JAKITS: Both of you facetime No bullshit $1000 a piece
- VICTIM 1: What do we have to do on FaceTime is my question
- JAKITS: Whatever i tell you
- JAKITS: Nothing nasty I ain't and don't like nasty
- JAKITS: If you're thinking about it, Then show me a close-up of both of your bottoms Simple It's a lot of money

***

- VICTIM1: We don't . Feel comfortable doing it[.]

35. In further communications recovered from Victim 1's phone that continued through on or about January 21, 2019, Jakits continued to tell Victim 1 that he would provide Victim 1, Victim 2 and the mother with a lot of money, claiming that he was a millionaire, if they were "up for trying again" or if Victim 1 would answer him. Victim 1 did not respond to any of Jakits' messages.

36. In January 2020, a subpoena was issued to Apple Inc. for information pertaining to telephone number (443) 742-1792. In response, Apple identified email addresses berniejakits@comcast.net and bernicjakits@me.com as being associated with the provided information. Your affiant subsequently obtained a search warrant for the content of the i-Cloud account associated with these email accounts/addresses and served the warrants on Apple, Inc. in April of 2020. Responsive information provided by Apple revealed numerous images of Victim 1 and Victim 2 stored in the content of the i-Cloud account as well as a photograph of Jakits'

Maryland Driver's License showing a date of birth of 6/1/1951. Specifically, the following 17 images were found to be present in the account:

- Image 1 – Photograph of a young Hispanic female lying naked on a sheet displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 2 – Photograph of a young naked Hispanic female bent over an object, possibly a bed. Your affiant was unable to conclusively identify the female as either Victim 1 or Victim 2, but did find a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 3 – Close up of a vagina. Your affiant was unable to identify the female, but did find a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 4 – Photograph of a young Hispanic female laying naked on a sheet displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 5 – Photograph of a young Hispanic female squatting naked displaying her breasts and vagina. Your affiant believes this to be Victim 1. While the female's face is not captured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 6 – Photograph of a young Hispanic female displaying her exposed breasts. Your affiant believes this to be Victim 1. While the female's face is not captured in the image a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 7 – Photograph of a young Hispanic female standing naked and showing her breasts. While the female's face is not captured in the photograph, text added to the image identifies the female photographed as Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 8 – Photograph of a young Hispanic female posing naked in mirror with breasts exposed. Your affiant believes this to be Victim 1. While the female's face is partially obscured in the image. a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 9 – Photograph of a young Hispanic female kneeling and wearing black bra and panties. Your affiant believes this to be Victim 1. While the female's face is obscured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Additionally, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 10 – Close up photograph of a female's buttocks while wearing a

black thong. Your affiant was unable to identify the female as either Victim 1 or Victim 2. However, your affiant observed a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.

- Image 11 – Close up photograph of a vagina. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant found a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 12– Photograph of a young Hispanic female kneeling and wearing black bra and panties. Your affiant believes this to be Victim 1. While the female's face is obscured in the image, a necklace similar in appearance to one worn by Victim 1 in other photographs is visible. Additionally, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 13 – Photograph of a young Hispanic female kneeling and wearing white bra and panties. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant observed a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 14 – Black and white photograph of a young female sitting on bathroom counter wearing thong panties. Although your affiant was unable to conclusively identify the female as either Victim 1 or Victim 2, a similar photograph was recovered from Victim 1's cellular telephone. Your affiant thus believes it is probable that the female in the photograph is either Victim 1 or Victim 2.
- Image 15 – Photograph of Victim 1 clothed displaying a school report card.
- Image 16 – Photograph of a young Hispanic female lying naked on a sheet displaying her breasts and vagina. Your affiant believes this to be Victim 1 based on a review of other known photographs of Victim 1. Furthermore, your affiant found a similar photograph on Victim 1's cellular telephone.
- Image 17 – Photograph of a young Hispanic female posing in a mirror wearing a black bra with a floral pattern. Your affiant was unable to identify the female as either Victim 1 or Victim 2. Your affiant found a similar photograph on Victim 1's cellular telephone and believes it is probable that the female in the photograph is either Victim 1 or Victim 2.

37. In June of 2020, your affiant conducted a telephonic interview with Victim 1 and her mother. Victim 1 confirmed to your affiant that she communicated with Jakits through "Text Now", a mobile messaging application on her phone.

38. In July 2020, a subpoena was served on Western Union for money transfer records pertaining to Jakits. Responsive information provided by Western Union revealed that Jakits sent $150 to Victim 1's grandmother on January 4. On January 11, 2019, Jakits sent $500 to Victim 1's grandmother. Jakits provided his telephone number as (443)742-1792.

39. In December 2020 the United States District Court for the District of Maryland issued a search warrant for Jakits' person and his residence, located at 780 Fairview Ave Apt F,

Annapolis, MD 21403, which was executed on December 10, 2020. During the execution of the search warrant, it was discovered that Jakits was traveling to Los Angeles, CA at the time of the execution. Further investigation determined Jakits was traveling on American Air Lines Flight 1165 from Regan National Airport to Los Angeles International Airport (LAX), and was scheduled to land at LAX at approximately 9:30am PST. Based on this information, your affiant contacted FBI Agents in Los Angeles, and upon Jakits arrival at LAX, he was met by Agents of the FBI, who advised him they had a search warrant for his person. Jakits was advised he was not under arrest. He agreed to accompany the agents to the FBI office in LAX where the search could occur. Once in the office, Jakits was provided with a copy of the search warrant, and he removed an Apple iPhone from his pants pocket and turned it over to the agents along with the password for the device. He further stated that he had a laptop computer and an iPad in his backpack. Jakits was advised of his Miranda rights verbally and in writing utilizing a standard FBI Form. Jakits stated he understood his rights and signed the aforementioned FBI Form. Jakits then provided both verbal and written consent to search both his Apple iPad and his Apple laptop. Based on that consent, agents conducted a manual review of the iPad in Jakits presence. That review led to the discovery of a photo vault application. When asked, Jakits provided the pass code for the photo vault application. In the application, FBI agents observed folders labeled with the names of Victim 1 and Victim 2. When FBI agents opened the folders, they observed sexually explicit photos of young females. A photo in the folder labeled with VICTIM 1's name showed a female holding what appeared to be a school transcript. A photo in the folder labeled with Victim 2's name depicted a female holding a piece of paper that displayed her date of birth, indicating her age as being 13 years old at the time the photograph was taken. The description of these images, as provided by the LA Agents, is consistent with photos that Victim 1 and Victim 2 sent to Jakits, as observed in the chat log on Victim 1's phone and in Jakits' iCloud account. Based on that similarity, your affiant has reason to believe that the sexually explicit photos that were found in these folders also depicted Victim 1 and Victim 2. At this time Jakits invoked his right to counsel and the interview and consent search of the iPad was terminated.

40. After finding what they believed to be child pornography on Jakits' iPad, the LA FBI Agents seized all of Jakits' devices and shipped them from the Los Angeles FBI to the Cincinnati FBI for further review and forensic examination. The LA Agents who seized Jakits' devices provided your affiant with identifying information pertaining to those devices, which is the identifying information of the SUBJECT DEVICES. The SUBJECT DEVICES have remained in

secure storage at the FBI Cincinnati office since they were received, and no further examination of the SUBJECT DEVICES has been conducted since the consent search of the iPad was terminated in LA.

VIII. CONCLUSION

41. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 2422(b) have been committed, and evidence of those violations is located on the SUBJECT DEVICES. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the SUBJECT DEVICES and the seizure of the items described in Attachment B.

Andrew D. McCabe
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 19th day of January 2021.

Elizabeth A. Preston Deavers
United States Magistrate Judge

io

ATTACHMENT A

Property to Be Searched

This warrant applies to the search of the following devices which are currently in the control of the Cincinnati FBI:

a. Apple iPad Pro, Serial Number, DMPWG0FTHPT4;

b. Apple Laptop Serial Number, C17N6MT86085;

c. Apple iPhone 12, serial number C392Q0T1N6XX.

ATTACHMENT B

Particular Things to be Seized

1. The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 2251(a) (production of child pornography); Title 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography); 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography); and 18 U.S.C. § 2422(b)(coercion and enticement):

a. Child pornography and child erotica.

b. Evidence of communications related to the production, possession, receipt, or distribution of child pornography and/or, the coercion or enticement of a minor to engage in illegal sexual activity.

c. Evidence that may identify any additional victims, co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

d. Evidence the user possessed, exchanged or requested visual depictions of minors, from other adults or minors themselves, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.

e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation.

f. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

g. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

h. Evidence of the lack of such malicious software.

i. Evidence indicating how and when the device was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.

j. Evidence indicating the device's user's state of mind as it relates to the crime under investigation.

k. Evidence of the attachment to the device of other storage devices or similar containers for electronic evidence.

l. Evidence of programs (and associated data) that are designed to eliminate data from the device.

m. Evidence of the times the device was used.

n. Records of or information about Internet Protocol addresses used by the device.

o. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

p. Contextual information necessary to understand the evidence described in this attachment.

q. Records, information, and items relating to violations of the statutes described above.

2. This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits,

and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

3. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

4. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.